



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/063,933	05/28/2002	Takayuki Sato	AT-0024US	7803

23419 7590 02/28/2007
COOLEY GODWARD KRONISH LLP
3000 EL CAMINO REAL
5 PALO ALTO SQUARE
PALO ALTO, CA 94306

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/063,933	SATO, TAKAYUKI	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 January 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15, 17 and 18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15, 17 and 18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>1/5/07</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05 January 2007 has been entered.
2. Claims 1-15, 17, and 18 have been presented for examination.
3. Claim 16 has been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments with respect to claims 1-15, 17, and 18 have been considered but are moot in view of the new grounds of rejection.
5. See further rejections that follow.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
7. Claims 1, 4, 5, 7, 13, 17, and 18 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,511,122 to Atkinson et al., hereinafter Atkinson.
8. As per claim 1, Atkinson discloses communication system that connects a first network and a second network for communication thereof, comprising:

a first interconnecting device (Figure 4, i.e. GW in subnet 1) connected to a first communication device (Figure 4, i.e. Host A) of said first network;

Art Unit: 2131

an authentication apparatus, positioned to isolate said first network from said second network (Figure 4 [block 116]), said authentication apparatus operable to perform authentication of authentication information received from said first interconnecting device and thereby operable to control whether or not communication between said first network and said second network is allowed (Figure 4 [blocks 106, 110], column 11, lines 1-27); and

an external recording device (column 12, lines 45-47, i.e. central directory) connecting to said first interconnecting device and operable to store authentication information of a user of said first communication device (column 12, lines 45-47, i.e. central directory storing hosts' authentication keys), said authentication information being used for authentication of the user by said authentication apparatus (column 11, lines 9-16, column 12, lines 38-47, i.e. authentication keys used to generate digital signature which is authenticated by the intermediary apparatus), wherein said first interconnecting device comprises:

an acquiring unit operable to acquire said authentication information of the user of said first communication device from said external recording device (Atkinson discloses that the terms gateway and intermediate router are interchangeable terms at column 9, lines 26-30. Atkinson further discloses at column 11, lines 9-14 that the intermediary router acquires the published to verify that the digital signature received is authentic. Finally at column 12, lines 45-47, Atkinson discloses that authentication keys (which are used to generate the digital signature used to authenticate the user) is published via a central directory service. Therefore, Atkinson teaches an acquiring unit at the interconnecting device (gateway) that obtains user authentication information (published authentication keys) from the external recording device (central directory service).); and

Art Unit: 2131

a transmit unit operable to transmit said authentication information acquired by said acquiring unit to said authentication apparatus (Figure 4 [blocks 16, 18, 100], column 9, lines 9-24, i.e. GW creates packets or fragments of authentication data and transmits to the intermediary device).

9. As per claims 4 and 13, Atkinson discloses an interconnecting device for connecting a first network and a second network to enable communication between a first communication device of said first network and a second communication device of said second network, the interconnecting device comprising:

an acquiring unit operable to acquire from a recording device, which is outside said interconnecting device, authentication information of a user of said first communication device for authentication of the user, by an authentication apparatus (Atkinson discloses that the terms gateway and intermediate router are interchangeable terms at column 9, lines 26-30. Atkinson further discloses at column 11, lines 9-14 that the intermediary router acquires the published to verify that the digital signature received is authentic. Finally at column 12, lines 45-47, Atkinson discloses that authentication keys (which are used to generate the digital signature used to authenticate the user) is published via a central directory service. Therefore, Atkinson teaches an acquiring unit at the interconnecting device (gateway) that obtains user authentication information (published authentication keys) from the external recording device (central directory service).),

wherein said authentication apparatus is positioned to isolate said first network from said second network (Figure 4 [block 116]); said authentication apparatus operable to perform authentication of authentication information received from said interconnecting device and

Art Unit: 2131

thereby operable to control whether communication between said first network and second network is allowed (Figure 4 [blocks 106, 110], column 11, lines 1-27); and

a transmit unit connected to said acquiring unit and operable to transmit said authentication information received by said acquiring unit to said authentication apparatus (Figure 4 [blocks 16, 18, 100], column 9, lines 9-24, i.e. GW creates packets or fragments of authentication data and transmits to the intermediary device);

wherein said interconnecting device (Figure 4 [block 18], i.e. GW in subnet 1) is located between said first communication device (Figure 4 [block 10], i.e. host A) and said authentication apparatus (Figure 4 [blocks 106, 116]).

10. Regarding claim 5, Atkinson teaches wherein said acquiring unit comprises a reading unit operable to read said authentication information from a non-volatile memory that comprises said recording device storing said authentication information (column 12, lines 45-47, i.e. Atkinson discloses that the authentication information is published on a central directory service, which is a computing device that comprises non-volatile memory).

11. Regarding claim 7, Atkinson discloses wherein said acquiring unit further acquires identification information of said authentication apparatus from said recording device (Atkinson discloses that the terms gateway and intermediate router are interchangeable terms at column 9, lines 26-30. Atkinson further discloses at column 11, lines 9-14 that the intermediary router acquires the published to verify that the digital signature received is authentic. Finally at column 12, lines 45-47, Atkinson discloses that authentication keys (which are used to generate the

Art Unit: 2131

digital signature used to authenticate the user) is published via a central directory service.

Therefore, Atkinson teaches an acquiring unit at the interconnecting device (gateway) that obtains user authentication information (published authentication keys) from the external recording device (central directory service).), and said transmit unit transmits said authentication information to said authentication apparatus (Figure 4 [blocks 16, 18, 100], column 9, lines 9-24, i.e. GW creates packets or fragments of authentication data and transmits to the intermediary device).

12. Regarding claim 17, Atkinson discloses wherein said authentication (Figure 4 [blocks 106, 116]) is located between said interconnecting device (Figure 4 [block 18], i.e. GW in subnet 1) and said communication device (Figure 4 [blocks 52, 54], i.e. host B).

13. Regarding claim 18, Atkinson discloses wherein said first interconnecting device (Figure 4 [block 18], i.e. GW in subnet 1) prevents said first communication device (Figure 4 [block 10], i.e. host A) from directly transmitting authentication information to said second interconnecting device (Figure 4 [blocks 106, 116], i.e. all communication from host A must go through GW in subnet 1).

Claim Rejections - 35 USC § 103

14. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15. Claims 2, 3, 6, 8, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson in view of U.S. 6,934,745 to Krautkremer, hereinafter Krautkremer.

Art Unit: 2131

16. Regarding claims 2, 3, 8, and 14, Atkinson discloses wherein said second interconnecting device includes a receive unit operable to receive said authentication information from said first interconnecting device (Figure 4 [blocks 34], column 11, lines 19-27, GW in subnet 2 receives packets/fragments with digital signature)); an authentication unit connected to said receive unit and operable to authenticate said authentication information received by said receive unit (Figure 4 [blocks 124], column 11, lines 19-27, i.e. the authentication process may be repeated by each intermediary router or gateway);

17. Atkins does not teach a setting unit connected to said authentication unit and operable to allow communication between said first communication device and said authentication apparatus when the authentication by said authentication unit is successful; wherein said acquiring unit of said first interconnecting device is further operable to acquire bandwidth information from said external recording device; said transmit unit of said first interconnecting device is further operable to transmit said bandwidth information acquired by said acquiring unit to said authentication apparatus; said receive unit of said authentication apparatus is further operable to receive said bandwidth information from said first interconnecting device; and said setting unit of said authentication apparatus is further operable to set a communication bandwidth between said first communication device and said authentication apparatus based on said bandwidth information.

18. Krautkremer discloses a setting unit connected to said authentication unit and operable to allow communication between said first communication device and said authentication apparatus when the authentication by said authentication unit is successful; wherein said acquiring unit of said first interconnecting device is further operable to acquire bandwidth information from said

Art Unit: 2131

external recording device; said transmit unit of said first interconnecting device is further operable to transmit said bandwidth information acquired by said acquiring unit to said authentication apparatus; said receive unit of said authentication apparatus is further operable to receive said bandwidth information from said first interconnecting device; and said setting unit of said authentication apparatus is further operable to set a communication bandwidth between said first communication device and said authentication apparatus based on said bandwidth information (Figures 1 [blocks 50, 61, 62] , 2, 3, 4 [blocks 50, 61, 62], 5 [blocks 50, 61, 62], column 4, line 12 to column 5, line 23, column 10, lines 28-60).

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to receive the client authentication data and configure the bandwidth for the connection between the two communicating devices, since Krautkremer states at column 2, line 56 to column 3, line 10 that such a modification would offer real-time monitoring, measurement and control of performance over the network. It would also allow providers to configure and maintain the network from a central location.

20. Regarding claim 6, Atkinson does not teach wherein said acquiring unit includes a receive unit operable to perform wireless communication with a wireless communication device that comprises said recording device storing said authentication information, and to receive said authentication information from said wireless communication device by the wireless communication.

21. Krautkremer discloses wherein said acquiring unit includes a receive unit operable to perform wireless communication with a wireless communication device that comprises said

Art Unit: 2131

recording device storing said authentication information, and to receive said authentication information from said wireless communication device by the wireless communication (column 8, lines 36-48).

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use wireless communications, since Krautkremer states at column 2, line 56 to column 3, line 10 that such a modification would offer a solution to circumvent traffic over hardwired lines of communication. It has also been held that it only requires routine skill in the art to make a device portable. See MPEP § 2144.04; see also *In re Lindberg*, 194 F.2d 732, 735, 93 USPQ 23, 26 (CCPA 1952).

23. Claims 9-12 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson in view of U.S. Patent No. 6,005,939 to Fortenberry et al., hereinafter Fortenberry.

24. Regarding claims 9 and 15, Atkinson does not teach a decryption unit connected to said acquiring unit and operable to decrypt encrypted authentication information.

25. Fortenberry discloses a decryption unit connected to said acquiring unit and operable to decrypt encrypted authentication information (column 6, lines 15-24, column 52-63).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a decryption unit to decrypt any authentication information that may be encrypt, since one of ordinary skill in the art would recognize the need to decrypt the authentication information before it was usable in generating the digital signature and Atkinson discusses encrypting authentication information at column 12, line 62 to column 13, line 8.

Art Unit: 2131

27. Regarding claims 10-12, Atkinson does not teach a processing unit connected to said transmit unit and operable to determine whether or not said authentication apparatus is allowed to authenticate the user, wherein said transmit unit transmits said authentication information to said authentication apparatus when said processing unit determines that said authentication apparatus is allowed to authenticate the user.

28. Fortenberry discloses a processing unit connected to said transmit unit and operable to determine whether or not said authentication apparatus is allowed to authenticate the user, wherein said transmit unit transmits said authentication information to said authentication apparatus when said processing unit determines that said authentication apparatus is allowed to authenticate the user (column 6, lines 7-14, column 8, lines 7-14).

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a determination of whether the intermediary device is allowed to perform the authentication procedure, since Fortenberry states at column 1, lines 55-58 that such a modification provides for a consistent, secure, and redundancy free technique for performing user authentication.

Conclusion

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

31. The following patents are cited to further show the state of the art with respect to intermediary authentication, such as:

United States Patent No. 6,301,661 to Shambroom, which is cited to show enhanced security through an intermediary device when downloading executable content.

United States Patent No. 6,219,707 to Gooderum et al., which is cited to show an intermediary device separating two separate networks.

United States Patent Application Publication No. 2003/0014625 to Freed et al., which is cited to show securing communication through an intermediary device.

United States Patent No. 6,681,327 to Jardin, which is cited to show brokering secure communications via an intermediary device.

United States Patent No. 5,923,756 to Sharmbroom, which is cited to show enhanced security through an intermediary device when downloading executable content.

United States Patent No. 6,158,007 to Moreh et al., which is cited to show a securing data via middleware.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.


33. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

34. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf


AYAZ SHEKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100